UMTS에서 네트워크 영역 보안과 IMS 보안

신상욱 | 부경대학교 공과대학 전자컴퓨터정보통신공학부
류희수 | ETRI 정보보호연구본부 정보보호기반연구팀 선임연구원, 팀장

1. 서론

UMTS(Universal Mobile Telecommunications System)는 IMT-2000이라고 불리는 ITU(International Telecommunication Union)에 의해 정의된 프레임워크 내에서 개발되고 있는 새로운 3세대 무선 셀룰러 통신시스템의 하나이다. UMTS는 UTRA(UMTS Terrestrial Radio Access)라고 불리는 새로운 무선 인터페이스를 사용하여 증가된 용량과 더 커진 서비스 범위를 제공한다[32].

UMTS 시스템의 기본적인 무선, 네트워크, 서비스 파라미터들은 1998년 ETSI(European Telecommunications Standards Institute)에 의해 정의되었다. ETSI는 전세계 무선 통신 시장의 약 70%를 점유하고 전세계적으로 6억5천만명 이상의 사용자를 가지고 있는 2세대 GSM(Global System for Mobile communications)을 성공적으로 개발했었다. UMTS의 중요한 특성은 새로운 무선 액세스 네트워크가 진화된 GSM 핵심망(core network)에 연결된다는 것이다[32].

ETSI에서 UMTS 표준화 작업은 1998년 3GPP(3rd Generation Partnership Project)라 불리는 지역 표준화 단체의 세계적인 협력 기구로 이관되었다. 3GPP2(3rd Generation Partnership Project 2)라 불리는 표준화 단체들의 또다른 협력 기구는 CDMA2000이라 불리는 다른 3G 무선 인터페이스와 북미의 ANSI-41 표준으로부터 진화된 핵심망에 기반한 또다른 3세대 이동 셀룰러 시스템을 개발하고 있다.

GSM의 중요한 특징 중의 하나는 보안 특성이다[10,34]. UMTS 보안은 GSM의 연속선상에서 구성되며 새롭고 강화된 보안 특성들을 제공한다. UMTS 시스템의 보안구조는 무선 구간의 액세스 보안, 핵심망에서의 보안, 사용자 응용에서의 보안 등으로 분류할 수 있으며, 현재 무선 구간에서의 액세스 보안 부분은 거의 표준화가 완료되었다[3, 12]. 3GPP는 무선 구간에서 사용자와 네트워크 간의 상호 인증을 제공하고 암호화 키/무결성 키를 일치시켜주는 메커니즘으로 AKA(Authentication and Key Agreement)를 개발하였고[3], 국제적인 로밍에 필수적인 암호화와 무결성을 위한 함수로 각각 f8과 f9를 표준화하였다[7,8]. 또한 AKA 관련 함수 f0~f5에 대해서도 MILENAGE라는 예제 알고리즘 집합을 개발하여 사업자들을 위해 제공하였다[9].

본 고에서는 UMTS 핵심망 보안에 관한 표준 개발 동향을 분석한다. 또한 UMTS에서 IP 멀티미디어 서비스 제공을 위한 핵심망 부분인 IMS(IP Multimedia Subsystem)에서의 보안에 대해서 분석한다.

2. 네트워크 영역 보안 (Network Domain Security : NDS)

네트워크 영역 보안은 네트워크 개체들 사이의 통신에 대한 보안을 의미하며, MS(Mobile Station)은 네트워크 영역 보안에 의해 영향을 받지 않는다. 두 통신 개체는 한 운영자에 의해 관리되는 동일한 네트워크에 있을 수 있고, 또는 두 개의 다른 네트워크에 속할 수도 있다. 후자의 경우 즉 네트워크간 통신은 표준화된 기법을 요구하며 전자의 경우 많은 운영자들이 여러 제조업체에 의해 생산된 네트워크 개체를 가지기 때문에 네트워크 영역 보안에 관한 표준화는 많은 이점을 제공한다.

2세대 이동통신 시스템에서는 네트워크간 통신에 대해 암호학적 보안 메커니즘이 제공되지 않았다. GSM의 핵심망 부분은 공격자에 의해 사용될 수 있는 외부 인터페이스가 없는 "closed network"로 여겨졌다. GSM은 시그널링 메시지를 위해 MAP(Mobile Application Part)을 가진 SS7(Signaling System number 7) 프로토콜 스택을 사용한다. SS7 프로토콜의 복잡성과 구현의 제한된 가용성으로 인해 SS7에 관한 상세한 지식은 네트워크 운영업체의 내부인에게만 제한되었고, 이것은 잠재적인 위협을 줄이는데 도움을 주었다. 그렇지만 이러한 상황은 두 가지 이유로 인해 변하고 있다. 먼저 많은 수의 운영자들과 서비스 제공자들이 서로 통신하는 빈도가 증가하고 있으며, 또한 SS7 네트워크가 IP 네트워크로 대체되고 있다. IP 네트워크의 도입은 많은 이점을 제공하지만 동시에 많은 보안상의 문제점을 야기한다. 따라서 네트워크간의 시그널링에 대한 보호 메커니즘의 부재는 점점 더 심각한 보안상의 위험을 초래할 수 있다.

3GPP Release 99 표준 문서들의 주요 부분은 완전히 새로운 무선 액세스 기술의 도입에 관해 초점을 맞추었지만 핵심망 부분은 기존의 GSM 문서의 확장이었다. 이것이 Release 99에서 핵심망 시그널링에 대한 보호 메커니즘이 도입되지 않은 주요한 이유이다. 네트워크 영역에 대한 보호 메커니즘은 Release 4에서부터 시작되었다[11, 33].

SS7 시그널링의 mobile specific part는 MAP이라고 불린다[2]. SS7 네트워크에서 모든 통신을 보호하기 위해 MAP 프로토콜만을 보호하는 것은 충분하지 않지만 이동통신 관점에서 MAP은 필수적으로 보호되어야 하는 부분이다. 예로 무선 구간을 보호하기 위한 세션 키와 다른 인증 데이터들이 MAP으로 전달된다. 반면에 SS7을 위한 보안 프로토콜은 요구된 개발일정 안에 완료되는 것이 불가능한 작업이다. 이러한 이유로 인해 3GPP는 MAP에 한정된 보안 메커니즘을 개발하였다. MAPSEC이라 불리는 이 메커니즘들은 응용계층에서 MAP 메시지를 보호하며, TS 33.200[4]과 TS 29.002[2] 문서에 기술되어져 있다.

IP 기반 네트워크를 위한 많은 보안 프로토콜들이 현재 IETF(Internet Engineering Task Force)에 의해 표준화되어지고 있기 때문에 3GPP를 위해 완전히 새로운 프로토콜을 개발할 필요는 없지만, 3GPP 네트워크에서 IP 기반 통신을 보호하기 위해 IETF 프로토콜들을 어떻게 사용할 것인지에 관해, 합의에 도달하는 것은 중요한 문제이다. TS 33.210[6] 문서가 이에 관한 내용을 기술하고 있으며, 3GPP에서 사용되는 IETF의 주요 보안 프로토콜은 IPsec 프로토콜이다[15, 16].

또한 3GPP는 MAP 프로토콜이 어떻게 IP 위에서 동작하는지를 규정하며, 이 경우 MAP을 보호하기 위해 두 가지 방안, MAPSEC을 사용하는 것과 IPsec을 사용하는 것이 존재한다. IPsec은 IP 계층에서 수행되기 때문에 MAPSEC보다 더 하위 계층의 헤더들을 보호할 수 있다는 이점을 가진다.

2.1 MAPSEC

MAPSEC은 기본적으로 다음과 같이 동작한다. 평문의 MAP 메시지는 암호화되어 새로운 MAP 메시지의 'container' 부분에 주입되고, 동시에 암호학적 체크섬, 즉 원래의 평문 MAP 메시지에 대한 메시지 인증코드(Message Authentication Code : MAC)가 새로운 MAP 메시지에 포함된다. 암호화와 MAC을 사용하기 위해서는 키가 필요하며, MAPSEC은 IPsec에서 SA(Security Association) 개념을 가져온다. SA는 암호 키 그리고 키의 라이프타임, 알고리즘 식별자와 같은 관련 정보를 포함한다. MAPSEC의 SA는 IPsec의 SA와 유사하지만 동일하지는 않다.

3GPP Release 4는 운영자들 사이에 SA가 어떻게 교환되는지를 정의하지 않는다. 이것은 SA들이 네트워크 개체에 수동으로 구성된다는 것을 함축한다. MAPSEC에 대한 자동화된 키 관리는 3GPP Release 6에서 명시될 것이며, 3GPP는 자동화된 MAPSEC 키 관리를 위해 KAC(Key Administration Centre)라는 새로운 개체를 도입한다. KAC들은 IETF IKE(Internet Key Exchange)[17] 프로토콜을 사용하여 SA를 설정한 후 네트워크 개체들에게 SA를 분배한다. 같은 보안영역(security domain)에서의 모든 개체들은 같은 SA를 공유하며 또한 같은 보안정책(security policy)을 공유한다.

MAPSEC은 no protection, integrity protection only, encryption with integrity protection의 3가지 보호 모드를 가진다. Encryption with integrity protection에서 MAP 메시지는 다음의 구조를 가진다.

Security Header f6(Plaintext) f7(Security Header f6(Plaintext))

여기서 암호화 알고리즘인 f6은 AES(Advanced Encryption Standard) CTR(counter) 모드를 사용하고, MAC 알고리즘인 f7은 AES에 기반한 CBC-MAC 기법을 사용한다. security header는 SPI(Security Parameter Index), 전송 네트워크 식별자 등과 같이 수신측에서 메시지를 처리하기 위해 필요한 정보를 포함한다.

MAPSEC에서는 성능상의 이유로 인증 데이터 전송과 같이 중요한 몇 가지 MAP 메시지만을 보호한다.

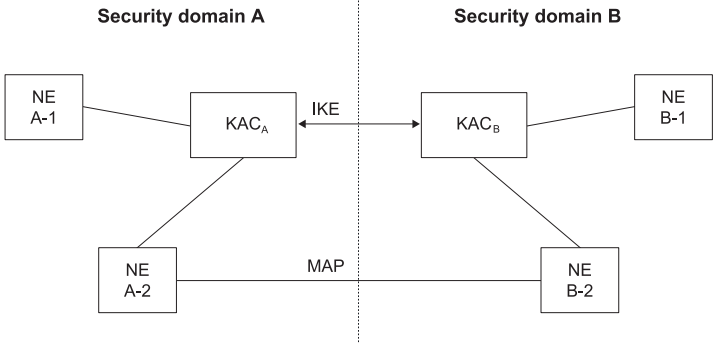


그림 1. MAPSEC을 위한 자동화된 키 관리

2.2 IPsec 기반 메커니즘

IPsec 기반 메커니즘에서 외부 네트워크로의 모든 control plane IP 통신은 SEG(Security Gateway)라 불리는 새로운 개체를 통해 수행되어야 한다. 이 게이트웨이는 IPsec SA 교환을 위해 IKE 프로토콜을 사용한다. SEG와 MAPSEC KAC 사이의 중요한 개념적 차이점으로 KAC는 외부 네트워크의 KAC와 SA를 협상하여 네트워크 개체에게 분배하기만 하고 실제 MAP 메시지의 송수신은 다른 네트워크 개체들에 의해 수행되지만 SEG는 외부 네트워크의 SEG와 SA를 협상하여 자신이 이 SA를 사용하여 외부 네트워크와 통신한다는 것이다. 3GPP Release 5에서 IKE는 pre-shared secret에 기반한 방식을 사용하며, PKI(Public Key Infrastructure)의 지원은 추후에 추가될 것이다. SEG는 SA DB와 보안 정책 DB 모두를 포함하며, 물리적으로 보호되어야 한다.

IPsec이 너무 많은 선택 사항을 가지기 때문에 완전한 상호 호환성을 제공하는 것이 어렵다. 따라서 3GPP에서는 이 문제를 해결하기 위해 다음과 같이 IPsec의 선택 사항을 줄였다.

- 패킷 보호를 위해 ESP(Encapsulating Security Payload)[18]만을 사용하고, AH(Authenticated Header)[19]는 사용하지 않는다.
- ESP는 항상 tunnel 모드로 사용된다.
- ESP에서 암호화 알고리즘으로 3DES 알고리즘을 사용하고, 무결성/인증 알고리즘으로 HMAC-SHA-1 알고리즘을 사용한다.
- IKE는 pre-shared secret에 기반한 main mode로 사용된다.

그림 2에서 Za 인터페이스는 반드시 구현되어야 하며, Zb 인터페이스는 구현에서 선택사항이다. 또한 Za 인터페이스에서 ESP는 항상 암호화와 인증을 모두 제공해야 하며, Zb 인터페이스에서는 인증은 항상 제공되어야 하지만 암호화는 선택 사항이다.

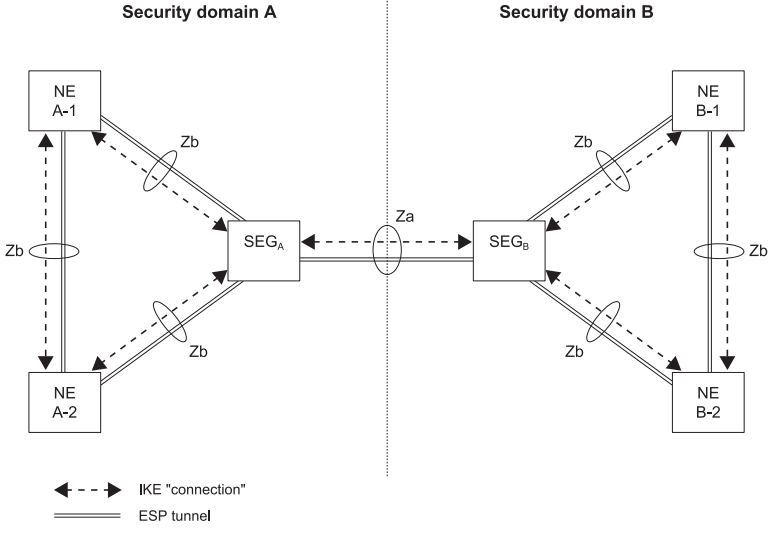


그림 2. IP 기반 제어 메시지를 위한 네트워크 영역 보안

3. IMS(IP Multimedia Subsystem) 보안

3.1 IMS 개요

IP 멀티미디어 서브시스템(IMS)[1]은 UMTS내의 핵심망 서브시스템으로 화상 회의, 스트리밍 서비스, 채팅과 같은 멀티미디어 세션을 개시, 종료, 수정하기 위해 현재 IETF에서 개발되고 있는 SIP(Session Initiation Protocol)[20]를 사용한다. 또한 IMS는 세션 파라미터를 명시하고 사용되는 코덱(codec)을 협상하기 위해 IETF의 SDP(Session Description Protocol)[21]를 사용한다. SIP는 UDP(User Datagram Protocol)와 TCP(Transmission Control Protocol) 같은 다양한 IP 전송 프로토콜 위에서 동작한다.

IMS 아키텍처는 TS 23.228[1]에 명시되어 있으며 UMTS 패킷 도메인 위에 구축되지만, IMS의 아키텍처는 향후에 UMTS 패킷 도메인에 의해 제공되는 것 이외의 IP connectivity를 위한 메커니즘을 사용할 수 있도록 설계된다. "액세스 네트워크 독립성"으로 불리는 이 요구 사항을 만족시키기 위해 IETF 메커니즘에 크게 의존한다. 3GPP는 3GPP 요구사항을 만족하는 IETF 표준을 제공하도록 IETF 표준 개발 작업에 매우 적극적으로 참여하고 있다.

SIP는 매우 일반적인 IETF 아키텍처에 기반하고 hop-by-hop 보안, end-to-middle 보안, end-to-end 보안의 다양한 신뢰 모델이 정의될 수 있다. 따라서 IETF SIP WG은 SIP의 다양한 사용 시나리오에 적용할 수 있는 다양한 보안 메커니즘을 정의하고 있다. 예로 보안 메커니즘들은 인증, 암호화, 무결성, 재연 방지 등의 서비스를 제공한다. SIP request와 response는 메시지의 일부가 라우팅 목적 등을 위해 프락시에서 활용 가능해야 하기 때문에 end-to-end 기반에서 완전히 암호화되거나 무결성 보호될 수 없다. SIP를 보호하기 위해 응용계층에서 HTTP (HyperText Transfer Protocol) 인증[25]과 S/MIME(Secure/Multipurpose Internet Mail Extensions)[35]을 사용하는 것이 가능하다. S/MIME은 공개키 인증서에 기반하고 어떤 경우에는 매우 큰 메시지를 생성한다는 단점을 가진다. 또한 좀더 하위의 전송계층과 네트워크 계층에서 전체 SIP 메시지를 보호하기 위해 TLS(Transport Layer Security)[36] 또는 IPsec을 사용하는 것도 가능하다. IMS에서 UDP와 TCP가 모두 사용되지만 UDP가 디폴트 프로토콜이고 TCP는 큰 메시지에 대해서만 사용된다. TLS는 TCP 위에서만 사용될 수 있고 공개키 인증서를 요구하기 때문에, TLS는 고려에서 배제된다.[11]

3GPP에서 IMS 보안에 관한 작업은 2000년 8월부터 시작되어 현재까지 계속 진행되고 있다. 3GPP는 SIP 보호를 위해 IETF와 긴밀한 협력 관계를 갖고 작업하고 있으며, HTTP Digest가 3GPP 일정 안에 종료될 수 없기 때문에 3GPP의 개발 일정을 고려하여 IPsec을 적용하는 것에 관해 작업하고 있다. 현재 IMS 보안에 관한 내용은 TS 33.203에서 정의하고 있다. SIP에서 인증은 IETF RFC 3310[26]에 명시된 Digest AKA 메커니즘을 이용하고, 홈망의 S-CSCF(Serving Call Session Control Function)에서 수행된다. 그리고 SIP 메시지에 대한 무결성 보호는 IPsec ESP를 사용하며, hop-by-hop 형태로 보호한다. UE와 네트워크 사이의 알고리즘 협상은 IETF RFC 3329[29]에 명시된 SIP를 위한 보안 메커니즘 협상 메커니즘을 사용하고, 홈망에서 방문망으로 키 전송은 IPsec ESP에 의해 보호된다. IMS 보안은 네트워크내의 다른 보안과 독립적이다.

3.2 IMS를 위한 보안 아키텍처

3GPP IMS 보안 아키텍처는 TS 33.203[5]에 명시되어 있다. 3GPP IMS 가입자는 하나의 IMPI(IP Multimedia Private Identity)를 가지며, 적어도 하나의 IMPU(IP Multimedia PUblic identity)를 가진다. IMPI에 관련된 공유 비밀키가 ISIM과 HSS(Home Subscriber System)에 저장된다. IMS 가입자가 멀티미디어 세션에 참여하기 위해서는 IMS에 적어도 하나의 IMPU를 등록해야 한다. IMPI는 인증을 위해서만 사용된다. HSS는 S-CSCF에게 가입자 인증을 위임하지만, 키와 인증 데이터를 생성할 책임이 있다.

IMS 보안 아키텍처에 관련하여 4개의 IMS 개체가 존재한다.

- UE(User Equipment) : SIP 사용자 에이전트(UA) 그리고 IMS 보안 정보를 포함한 애플리케이션인 ISIM(IMS Subscriber Identity Module)에 기반한 스마트 카드를 포함한다. ISIM은 USIM과 데이터와 함수를 공유하지 않는 다른 애플리케이션일 수 있다. 또는 USIM과 데이터와 함수를 공유하거나 USIM을 재사용할 수도 있다. IMPI 당 하나의 ISIM만이 할당된다.
- P-CSCF(Proxy Call Session Control Function) : outbound SIP 프락시로 동작한다. UE에서 UA에 대해 방문망에서 첫 번째 접속 지점이 되고, SIP request를 I-CSCF로 발송한다.
- I-CSCF(Interrogating Call Session Control Function) : 홈망에서 접속 지점이고 SIP 프락시로 동작한다. SIP request 또는 response를 S-CSCF로 발송한다.
- S-CSCF(Serving Call Session Control

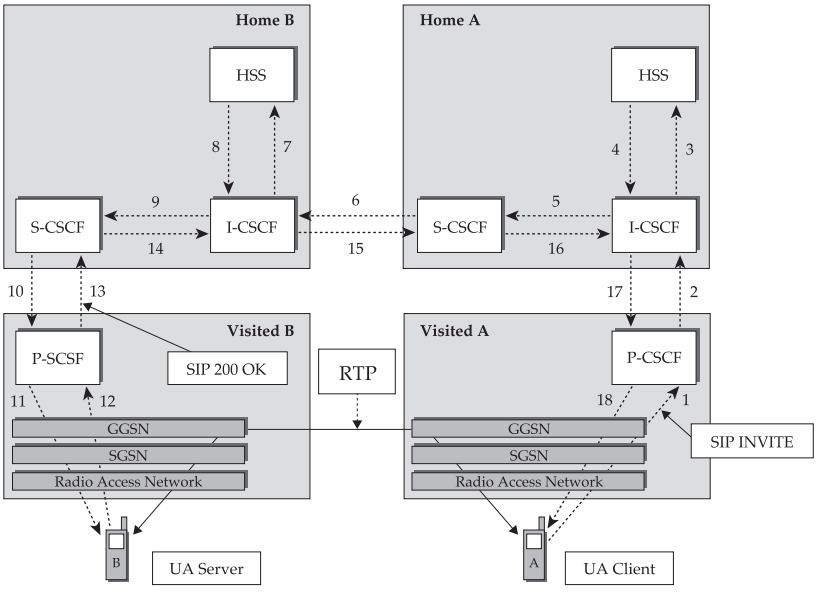


그림 3. IMS에서 세션 설정 시나리오

Function) : SIP registrar, SIP 프락시 서버, SIP UA로 동작한다. UE가 세션 설정을 위해 SIP INVITE 메시지를 전송할 수 있기 전에 먼저 S-CSCF에 자신의 IMPU를 등록해야 한다. IMPU 등록은 홈망으로 SIP REGISTRATION 메시지를 전송함으로써 UE에 의해 수행된다.

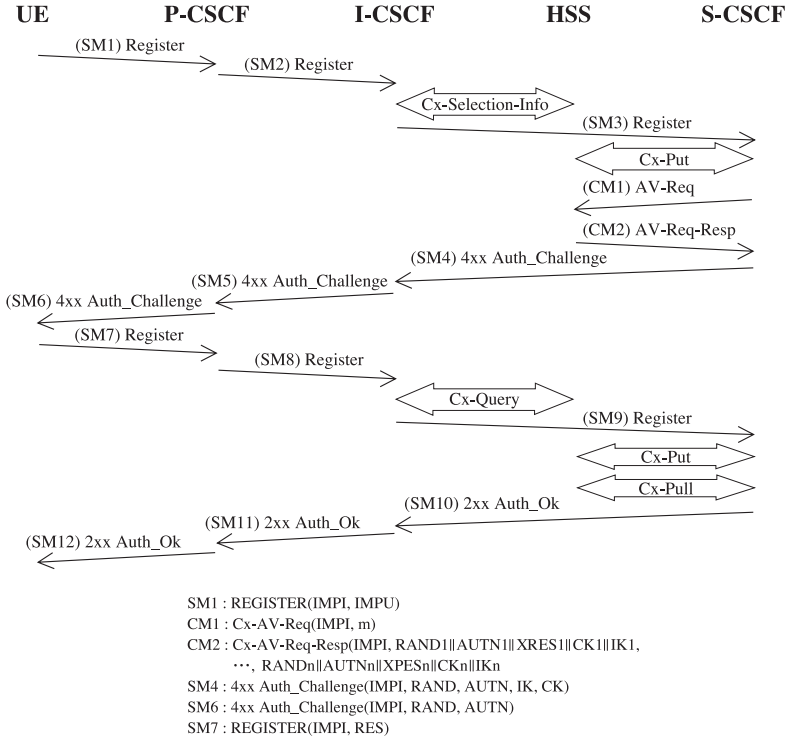
세션은 SIP INVITE 메시지를 사용하여 셋업된다. 그림 3은 3GPP 네트워크에 위치한 두 UE들 사이에 SIP INVITE 메시지가 전송되는 시나리오를 보여준다. 홈망 A의 UE A로부터 INVITE 메시지가 P-CSCF를 통해 I-CSCF에게 전달된다. I-CSCF가 HSS에게 메시지를 전달하면, HSS는 사용자가 등록된 S-CSCF를 찾는다. 유사한 과정이 홈망 B에서도 수행되며, INVITE는 UE B에 최종 전달되어 세션이 설정된다. 그 이후 IETF의 RTP(Realtime Transport Protocol)[22]와 같은 프로토콜을 사용하여 세션을 시작할 수 있다.

3.3 IMS의 보안 메커니즘

IMS 가입자는 개인 식별자 IMPI를 가지며, 모든 가입자 관련 데이터는 HSS에 저장된다. 사용자 등록과정 동안 가입자 데이터는 HSS로부터 S-CSCF에 전달된다. S-CSCF는 사용자의 액세스를 허용하기 전에 이 가입자 데이터와 사용자에 의한 request를 검증한다. 등록과정은 그림 4에 보여진다. SM1 메시지로 UE가 REGISTER 메시지를 전송하면, 이 메시지는 S-CSCF로 전달된다. IMS를 위한 인증과 키 일치는 UMTS 액세스 보안을 위한 AKA에 기반한다. UE가 등록을 요청하면, HSS가 인증을 위한 시도 값을 생성하여 S-CSCF에게 전달한다. S-CSCF는 SM4에서 SM6 메시지로 P-CSCF와 UE에게 전달한다. UE는 인증시도 값이 유효한지 검증한 후 SM7 메시지로 S-CSCF에게 응답 값을 반환한다. S-CSCF는 수신한 응답 값을 통해 가입자를 인증한다. 이것은 인증이 방문망으로 위임되는 UMTS 구조와 다르다. 따라서 이 구조는 P-CSCF에 대한 신뢰를 어느 정도 줄여준다. 홈망에서 S-CSCF는 언제든지 사용자 재인증을 요구할 수 있다.

사용자가 성공적으로 인증되고 UE가 200 OK 메시지를 수신하면, UE와 P-CSCF 사이에 SIP 메시지 보호를 위한 SA(Security Association)가 설정된다. P-CSCF는 S-CSCF에 의해 전송된 SM5 메시지로부터 SIP 보호를 위한 무결성 키를 획득한다. 무결성 키가 S-CSCF에서 P-CSCF로 전달되기 때문에 이 메시지는 홈망과 방문망 사이에서 보호되어야 한다. 이것은 TS 33.210에 명시된 메커니즘을 사용하여 네트워크 사이에 IPsec tunnel을 설정함으로써 달성된다.

UE와 P-CSCF 사이에는 무결성 보호만이 적용되며, 이것은 과금 관점에서 중요하다. 기밀성 보호는 IMS에 적용되지 않지만, UE와 RNC 사이의 무선 구간은 UMTS 링크 계층에서 제공되는 기밀성 메커니즘이 사용될 수 있다. End-to-end 보안에 대해서는 IETF SRTP(Secure Real time Transport Protocol)[23]와 MIKEY(Multimedia Internet KEYing)[24]가 RTP를 보호하고 키 관리 기법을 제공하기 위해 사용될 수 있다. 무결성 보호를 위해 사용되는 프로토콜은 IPsec ESP이다. IPsec ESP를 위한 SA는 IKE 또는 'manual keying'으로 생성될 수 있다. IKE 구현이 매우 복잡하기 때문에 단말기에서 수행하는 것이 불가능하므로, 'manual keying'이 IMS에 사용된다. 하지만 여기서 'manual'의 의미는 IPsec에서의 용어로써 잘못 이해될 수 있다. 실질적으



SM1 : REGISTER(IMPI, IMPU)
CM1 : Cx-AV-Req(IMPI, m)
CM2 : Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,
…, RANDn||AUTNn||XPESn||CKn||IKn
SM4 : 4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)
SM6 : 4xx Auth_Challenge(IMPI, RAND, AUTN)
SM7 : REGISTER(IMPI, RES)

그림 4. IMS에서 성공적인 등록과정

로 키 관리는 아래에 기술되는 것처럼 AKA 프로토콜에 의해 제공되는 자동화된 방법이다. SIP 계층에서 IPsec 계층으로 키와 다른 정보를 전송하기 위해 local API(Application Programming Interface)가 사용된다.

3.3.1 HTTP Digest AKA를 사용한 인증

SIP는 HTTP 프레임워크에 기반하므로 HTTP의 인증 프레임워크를 상속받는다. 그렇지만 HTTP Basic 인증이 패스워드를 평문으로 전송하는 것으로 인해 안전하지 않은 프로토콜이기 때문에 IETF SIP WG은 이 인증 프로토콜의 사용을 금지하고 있다. 따라서 SIP에서는 HTTP Digest 인증만이 허용된다. AKA에서 파라미터 RES는 평문으로 전달되더라도 AKA 프로토콜은 안전하기 때문에 HTTP Basic 인증과 AKA를 결합하여 사용하는 것은 어떤 취약점도 유발하지 않는다. 하지만 3GPP는 가능한 한 IETF와 호환되는 것을 목표로 하기 때문에 HTTP Basic 인증을 사용하지 않는다.

HTTP Digest와 AKA 프로토콜을 결합하여 사용하는 것은 다음처럼 동작한다. HTTP Digest는 S-CSCF에서 UE로 인증 시도 값을 전송하기 위해 사용된다. 이 메시지는 P-CSCF를 위한 인증 시도 값, 보안 메커니즘 식별자, 무결성 키를 전송하는 WWW Authenticate 헤더를 포함한다. UE가 인증 시도 값을 수신하면 먼저 MAC 값이 정확한지를 검증한 후

sequence number가 유효한 범위 안에 있는지를 검사한다. 이 검사가 성공하면 UE는 시도 값과 ISIM에 저장된 공유 비밀키에 기반하여 인증 응답 값 RES를 계산한다. RES는 HTTP Digest 프레임워크에서 패스워드로 취급되고, RES를 입력으로 하는 AKAv1 MD5를 사용하여 응답이 계산된다. S-CSCF는 XRES(expected RES)에 기반하여 유사하게 계산하여 검사를 수행한다.

3.3.2 IPsec ESP를 사용한 무결성 보호

IPsec ESP는 UE와 P-CSCF 사이에 transport mode로 IMS에 적용된다. UE와 P-CSCF 사이의 SA 쌍은 인증과정 동안 동시에 생성된다. 재연 공격(replay attack)을 방지하기 위해 IPsec ESP anti replay 서비스가 사용된다. 더욱이 두 SA에서 무결성 키가 동일하기 때문에 각 SA에 대해 SPI가 다르다는 것을 보장함으로써 reflection 공격에 대한 보호가 달성된다. 사용자로부터 비롯된 SIP 시그널링은 과금을 위한 기본 데이터로 사용되기 때문에 NULL 인증 알고리즘의 사용을 금지한다. 인증 알고리즘으로 HMAC-MD5-96[27] 또는 HMAC-SHA-1-96[28]이 사용된다.

SA는 정상적인 IPsec 선택자, 즉 출처와 목적지 IP 주소, 출처와 목적지 포트 번호에 연결된다. IMS에서 허용되는 전송 프로토콜은 UDP와 TCP이다.

4. 결론

3세대 이동통신 시스템의 무선 구간의 액세스 보안에 관한 표준은 3GPP와 3GPP2에서 개발이 거의 완료된 상태이며, 현재는 네트워크 영역에서의 보안에 관해 표준 개발을 진행 중에 있다. 본 고에서는 3GPP에서 표준화 진행 중인 네트워크 영역 보안과 IMS 보안의 주요 특징들을 분석하였다.

UMTS에서 다음의 release에 관한 작업을 현재 지속적으로 수행하고 있다. 새로운 UMTS release는 새로운 보안 특성들을 도입할 것이다. 이들 보안 특성들은 새롭게 도입될 서비스, presence 서비스, push 서비스, 멀티캐스트/브로드캐스트 서비스 등을 보호하기 위해 도입될 것이다.

향후에는 이동 셀룰러 시스템이 WLAN(Wireless Local Area Network)과 같은 다양한 무선 액세스 네트워크와 연동되어야 할 것이다. 사용자 측면에서 monolithic terminal의 개념이 희미해지고 있으며, 단거리 무선 링크에 의해 구성요소들이 상호 연결된 분산 단말 구조가 대두되고 있다. 이러한 새로운 발전 흐름은 UMTS 보안 구조에도 새로운 문제들을 제기한다. 이러한 이슈들을 해결하기 위해 유럽에서는 SHAMAN(Security for Heterogeneous Access in Mobile Application and Networks)이라는 협력 연구 프로젝트를 진행하고 있다[13]. 또한 이동통신 분야에서 향후 연구주제를 파악하기 위해 EU의 6th Framework Programme의 일부로 PAMPAS(Pioneering Advanced Mobile Privacy and Security)라는 프로젝트가 수행되고 있다[14].

국내의 경우 3세대 이동통신 시스템의 보안에 관한 연구가 미진하여 보안 표준 개발에 주도적으로 참여하지 못하였지만, 새로운 서비스의 도입과 이종 네트워크와의 연동과 같은 새로운 이슈들에서의 보안 문제에 관해서는 연구개발에 적극적으로 투자하여 표준화 활동에 주도적으로 참여해야 할 것으로 사료된다.

○ 참고문헌

[1] 3GPP TS 23.228 : IP Multimedia Subsystem (IMS), Stage 2

[2] 3GPP TS 29.002 : Mobile Application Part (MAP) specification

[3] 3GPP TS 33.102 : Security architecture

[4] 3GPP TS 33.200 : Network domain security: MAP application layer security

[5] 3GPP TS 33.203 : Access security for IP-based services

[6] 3GPP TS 33.210 : Network domain security: IP network layer security

[7] 3GPP TS 35.201 : Specification of confidentiality and integrity algorithms: f8 and f9 specifications

[8] 3GPP TS 35.202 : Specification of confidentiality and integrity algorithms: KASUMI specifications

[9] 3GPP TS 35.205 ~ 35.208 : Specification of the MILENAGE Algorithm Set; An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*

[10] GSM 03.20 : Network related security features

[11] Boman, K.; Horn, G.; Howard, P.; Niemi, V. : UMTS security, IEE Electronics & Communication Engineering Journal, Oct 2002, Vol.14, Issue 5, pp.191- 204

[12] HORN, G., and HOWARD, P. : Review of third generation mobile system security architecture , Proc. ISSE 00, Barcelona, 27th-29th September 2000

[13] http://www.ist-shaman.org

[14] http://www.pampas.eu.org

[15] IETF RFC 2401 (1998) : Security Architecture for the Internet Protocol

[16] IETF RFC 2408 (1998) : Internet Security Association and Key Management Protocol (ISAKMP)

[17] IETF RFC 2409 (1998) : IKE : Internet Key Exchange

[18] IETF RFC 2406 (1998) : IP Encapsulating Security Payload (ESP)

[19] IETF RFC 2402 (1998) : IP Authentication Header

[20] IETF RFC 3261 (2002) : SIP : Session Initiation Protocol

[21] IETF RFC 2327 (1998) : SDP : Session description Protocol

[22] IETF RFC 1889 (1996) : RTP : a transport protocol for real-time applications

[23] IETF draft-ietf-avt-srtp-04 (2002) : The Secure Real Time Transport Protocol

[24] IETF draft-ietf-msec-mikey-01 (2002) : MIKEY : Multimedia Internet KEYing

[25] IETF RFC 2617 (1999) : HTTP Authentication : Basic and Digest Access Authentication

[26] IETF RFC 3310 (2002) : HTTP Digest Authentication Using AKA

[27] IETF RFC 2403 (1998) : The Use of HMAC-MD5-96 within ESP and AH

[28] IETF RFC 2404 (1998) : The Use of HMAC-SHA-1-96 within ESP and AH

[29] IETF 3329 (2003) : Security Mechanism

Agreement for SIP
[30] IETF RFC 2633 (1999) : S/MIME Version 3 Message Specification
[31] IETF RFC 3546 (2003) : Transport Layer Security (TLS) Extensions
[32] RICHARDSON, K. W. : UMTS overview , Electron. Commun, Eng. J., June 2000, 12, (3), pp.93–100
[33] Stefan Pütz, Roland Schmitz, Tobias Martin : Security Mechanisms in UMTS, DuD · Datenschutz und Datensicherheit 25 (2001) X, pp.1–10
[34] WALKER, M., and WRIGHT, T. : Security aspects, a chapter in Hillebrand, F. (Ed.) : GSM and UMTS : The Creation of Global Mobile Communication(John Wiley & Sons, 2002)